Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 1, January 2023
https://doi.org/10.47709/cnahpc.v5i1.2286

Submitted : May 02, 2023
Accepted : May 22, 2023
Published : May 24, 2023

Forensic Web Analysis on The Latest Version of Whatsapp Browser

Dicky Satrio Ikhsan Utomo[1)*], Yudi Prayudi [2)], Erika Ramadhani[3)]
[1)2)3)]Industrial Technology Faculty, Islamic University of Indonesia
[1)] 20917012@students.uii.ac.id, [2)] prayudi@uii.ac.id, [3)] erika@uii.ac.id

ABSTRACT

With the rapid growth of technology and the increasing number of smartphone users, social media applications have proliferated. Among them, WhatsApp has emerged as the most widely used application, with over a quarter of the world's population using it since 2009. To meet the increasing customer demands, WhatsApp has introduced a browser version, which has undergone continuous updates and improvements. The latest version of WhatsApp exhibits significant differences in features and settings compared to its predecessors, particularly in conversations, images, video recordings, and other aspects. Consequently, this research focuses on analyzing artifacts that can aid in forensic investigations. The study aims to extract artifacts related to conversation sessions, as well as media data such as audio files, contact numbers, photos, videos, and more. To achieve these objectives, various forensic tools will be employed to assist in the artifact search within the WhatsApp browser. The research adopts the NIST framework and utilizes forensic techniques like Autopsy and FTK Imager to read encrypted backup database files. These files contain valuable information such as deleted conversations, phone logs, photos, videos, and other data of interest. Analyzing the artifacts from the WhatsApp browser version contributes to forensic activities, providing valuable insights into the evidence that can be obtained from conversations and media files. By leveraging forensic tools and techniques, forensic practitioners can effectively retrieve and analyze data from the encrypted backup database files. In summary, this research explores the artifacts within the WhatsApp browser version, sheds light on its distinct features, and presents a forensic approach utilizing the NIST framework and forensic tools like Autopsy and FTK Imager to examine encrypted backup database files containing crucial deleted data, conversations, and media files.

Keywords: Artifact Investigation, WhatsApp web messenger, Digital forensics, Autopsy, FTK Imager, NIST.

1. INTRODUCTION

The application known as Whatsapp is a messaging exchange application on a smartphone platform owned by everyone. The Whatsapp application itself uses internet data packages to run the application. In this application, everyone can send messages, pictures, documents, contacts, videos, and current location being used, and other voice messages using a mobile phone number (Martínez-Comeche & Ruthven, 2023).

Whatsapp released its latest version named WhatsApp Web on January 22, 2015. This new product was created for users who use PCs/computers. Like WhatsApp for smartphone users, this feature uses the internet as the main messaging channel. WhatsApp will open an online portal provided by the domain. For those who want to open WhatsApp on a computer page, this is the goal of WhatsApp web. Bidirectional synchronization is used to open the Web version of WhatsApp. To enter this version of Whatsapp, users will scan the barcode for the authentication process. After that, it will automatically open the Whatsapp application according to the account associated with the cellular Whatsapp. Therefore, cellular Whatsapp users will still get conversation sessions, media files, and others that will also be displayed in the web version of Whatsapp (Qureshi & El-Alfy, 2019).

Digital evidence has become a major contributor to decision-making in many important cases over the past few decades. As technology continues to evolve, more cases will depend on digital evidence (Lakshmi & Rajeshrajesh, 2019). Digital evidence is a crucial factor in most legal cases. However, technological advancements that lead to the complexity of artifacts force researchers to establish sophisticated connections between findings and suspects for the acceptance of evidence in court. This journal examines whether existing forensic tools can provide digital evidence to provide additional support and correlation to traditional investigative methods. This primarily focuses on artifacts from popular applications around the world (Iqbal & Riadi, 2019).

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 1, January 2023
https://doi.org/10.47709/cnahpc.v5i1.2286

Submitted : May 02, 2023
Accepted : May 22, 2023
Published : May 24, 2023

Digital forensics is a discipline that can currently connect all activities that include cybercrime, network security, and system management (Montasari et al., 2018). Digital forensics has morphed quite rapidly and has been applied to all aspects of computer and forensic movements.

Mobile forensics is a branch of digital forensics that has substance to determine electronic devices and other moving media. Therefore, it serves as a reference for researchers to work on several mobile devices (Paligu et al., 2019).

The use of Whatsapp has become very popular worldwide and is one of the most widely used messaging applications by the public. The latest version of Whatsapp Web Browser allows users to access Whatsapp through a web browser on a computer or laptop. This allows users to have conversations and share files using Whatsapp without the need for a mobile device.

However, as with other messaging applications, the latest version of Whatsapp Web Browser can also be used for illegal purposes, such as committing crimes or sending inappropriate messages. Therefore, it is important to perform forensic analysis of digital data stored in the latest version of Whatsapp Web Browser to help with the investigation process and disclosure of crimes.

Additionally, the latest version of Whatsapp Browser allows users to make voice and video calls, which can generate important digital data in criminal investigations. Therefore, an effective method is needed to conduct forensic analysis on the digital data generated by voice and video calls in Whatsapp Browser.

In this context, Web Forensic Analysis on the Latest Version of Whatsapp Browser plays an important role in assisting the investigation and disclosure of crimes. Therefore, research on forensic analysis methods and techniques on the latest version of Whatsapp Browser is necessary to support law enforcement and cybersecurity activities.

To address various cybercrimes, a digital forensics expert is needed. Data recovery is one of the techniques that a digital forensics expert must master (Simanjuntak & Panjaitan, 2021). If data is damaged or lost, it is the job of a forensics expert to recover the lost or damaged data. Some data recovery tools used by digital forensics experts include Autopsy, FTK imager, TSK recover, Foremost & Testdisk(Zuhriyanto et al., 2020).

A single case experiment was conducted with WhatsApp Messenger and the Web Application to fill and investigate artifacts in Google Chrome storage. The findings were characterized and presented with their potential for use in forensic verification investigations. The storage location of the artifacts was organized, and systematic extraction, conversion, and presentation operations were performed. Additionally, proof of concept tools were developed for demonstration purposes. The results indicate that the WhatsApp Web IndexedDB storage can be used for time frame analysis, demonstrating its value in evidence verification(Vukadinovic, 2019).

This research will use the NIST (National Institute of Standards and Technology) framework, which has stages that provide a high-level strategic view of cybersecurity risk management organizational management, general cybersecurity activities, desired outcomes, and applicable references to continue case reconstruction and support anticipating various unwanted incidents to avoid disrupting the data and file extraction process. This framework can also use tools commonly used in investigations to efficiently extract most of the information (Paligu et al., 2019).

Tools are used to search for missing data files, such as JPG, MP4, PDF, PNG, Doc, Zip, Rar, and others. However, these tools have certain limitations, as when data is retrieved or recovered, damaged data can only be recovered but cannot be fully opened. Therefore, the required solution is to recover the data fully, so that lost or damaged data can be recovered and reopened just as before (Wijnberg & Le-Khac, 2021).

While WhatsApp Web has gained significant popularity and is widely used, there is a lack of in-depth research on the forensic analysis of digital data stored in this browser version. Investigating and disclosing crimes related to the use of WhatsApp Web Browser require effective forensic techniques and methods to extract and analyze the digital evidence stored within the application.

Additionally, with the latest version of WhatsApp Web Browser allowing voice and video calls, there is a need for an effective method to conduct forensic analysis on the digital data generated by these communication features. Understanding how to retrieve and analyze the relevant digital evidence from voice and video calls within the WhatsApp Web Browser can significantly support criminal investigations.

Furthermore, while various forensic tools are available for data recovery and analysis, there is a need for research that explores the limitations and capabilities of these tools in recovering and fully opening damaged or lost data files. Enhancing the capabilities of forensic tools, such as Autopsy, FTK Imager, TSK recover, Foremost, and Testdisk, to recover and open damaged data files can greatly benefit digital forensics experts in their investigative processes.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 1, January 2023
https://doi.org/10.47709/cnahpc.v5i1.2286

Submitted : May 02, 2023
Accepted : May 22, 2023
Published : May 24, 2023

The utilization of the NIST framework in the research is also a notable aspect, as further investigation is required to understand how this framework can effectively guide the forensic analysis process and provide a strategic view of cybersecurity risk management. Additionally, exploring the potential of proof of concept tools developed for forensic analysis purposes can contribute to the field of digital forensics.

The research gaps identified include the need for comprehensive forensic analysis of the latest version of WhatsApp Web Browser, the development of effective methods for analyzing digital data generated by voice and video calls, exploring the limitations and capabilities of forensic tools for data recovery, further understanding the application of the NIST framework in forensic analysis, and investigating the potential of proof of concept tools for digital forensics purposes. Addressing these research gaps can significantly contribute to the field of web forensic analysis and support law enforcement and cybersecurity activities.

2. METHOD

This methodology will involve several steps that can detail the systematic and orderly sequence of activities in obtaining digital artifacts in this research, with the aim of obtaining a solution that becomes the root of the purpose of this research. The methodology to be carried out can be seen in figure 1.

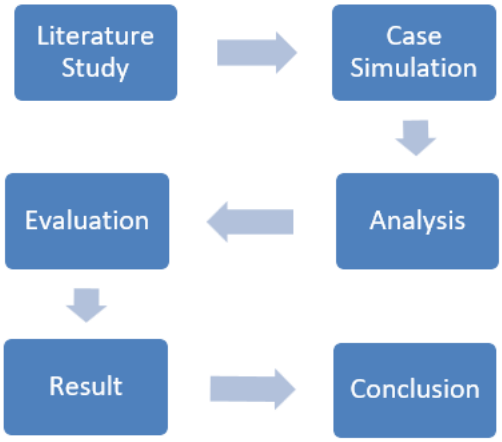

Fig.1 Research Methodology

This research will use the NIST (National Institute of Standards and Technology) method, which consists of four steps: collecting collections, examining data, analyzing the discovered artifacts, and finally creating a research findings report. The research flow or steps based on the NIST methodology are shown in Figure 2 below.

Fig. 2 NIST Framework

The collection phase aims to gather electronic evidence related to information security incidents. This includes collecting data, information, and records related to security incidents, such as log records, backup data, and so on.

The examination phase aims to analyze the electronic evidence that has been collected to ensure its validity and credibility (Khweiled & Jazzar, 2021). This phase includes examining the structure and format of the data, as well as examining the integrity and authenticity of the data.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 1, January 2023
https://doi.org/10.47709/cnahpc.v5i1.2286

Submitted : May 02, 2023
Accepted : May 22, 2023
Published : May 24, 2023

The analysis phase aims to gather relevant information and gain an understanding of the information security incident that occurred. This phase includes developing and testing hypotheses, as well as identifying the modus operandi of the perpetrator (Jafri et al., 2022).

The reporting phase aims to communicate the results of the analysis and examination process to the appropriate parties, such as management and information security teams (Riadi & Firdonsyah, 2018). This phase includes preparing reports and documentation, as well as delivering information in a clear and structured manner.

The collection, examination, analysis, and reporting method is a standard approach for conducting digital forensic analysis, including in cases of information security incidents (Rosselina et al., 2020). This method helps in collecting, examining, and analyzing electronic evidence in a structured and standardized way, ensuring accurate and accountable results. This method also assists in providing structured reporting and documentation that can be used as a reference in future efforts to prevent information security incidents (Shah et al., 2022).

To conduct this research effectively, reliable hardware and software are needed as research tools. The following are the tools and materials used in conducting the experimental research.

Table 1
Research Tools and Materials

No	Category	Spesification
1	Hardware	Laptop HP 15-ef2127 with the following specification: 1. Processor : AMD Ryzen 5500U Hexa-Core 2. Memory : 256 GB SSD / 8 GB RAM 3. OS: Windows 10 Home Insider 64-bit.
2	Software	Whatsapp Viewer, FTK Imager Tools, Sleuth Kit Autopsy Tools, Whatsapp Web.

3. RESULT & DISCUSSION

3.1 Collection

At the collection stage, hardware devices such as a PC and a smartphone were used, including:

a) PC1 - Windows 10 laptop formatted and installed with Google Chrome browser.
b) Phone1 - Android 10-Q smartphone that has been installed with WhatsApp.
c) Phone1 and PC1 added each other as contacts in the internal phonebook. Artifacts that are inherently found in storage are tested with the following steps:
d) WhatsApp Messenger is started on Phone1.
e) web.whatsapp.com is accessed through PC1.
f) The connection barcode in the PC browser is displayed to the Phone1 Messenger playback.
g) The connection between Phone1 and PC1 is left idle.
h) Artifacts are collected from the Chrome IndexedDB storage location on PC1.

3.2 Examination

Examination is an activity carried out with WhatsApp Messenger and Web Applications to create artifacts in IndexedDB storage. The activity is made according to observations of the user's common behavior with web browsers and communication messenger applications. When examining the stored activity information in WhatsApp Messenger and Web, the following activities are observed:

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 1, January 2023
https://doi.org/10.47709/cnahpc.v5i1.2286

Submitted : May 02, 2023
Accepted : May 22, 2023
Published : May 24, 2023

a) Text messages
b) Sending media messages including videos and pictures; images include jpeg files and files, gifs, and displaying transferred files
c) Voice calls
d) Video calls
e) Blocking and unblocking contacts

Displaying user contact info In addition, in the investigation and exploration carried out to find research potential, some user attendance records are observed. Based on the observed behavior, the following steps are used as the process:

a) Phone1 WhatsApp is connected to PC1 WhatsApp Web via a QR code.
b) Message "This is message 1" is sent from PC1 (Telepon1 connected) to Phone1.
c) Message "This is reply 1" is sent from Phone1 to PC1.
d) A sample video link is sent from PC1 to Phone1.
e) The sample video link is received from PC1 to Phone1.
f) The sample video is played on Phone1.
g) The sample video is played on PC1.
h) A video call request is sent from PC1 to Phone1. The call is answered and lasts for more than 5 seconds.
i) Phone1 is taken around twenty meters away (estimated to be about twenty steps) from PC1.
j) Phone1 is brought back to PC1.
k) Telepon1 is disconnected from PC1 and reconnected after 5 seconds.

3.3 Analysis

The artifacts created in computer storage by the WhatsApp Web application appear to provide broad information about user actions. This indicates a design intended to support different methods of information gathering.

It appears that actions taken with the WhatsApp Messenger application on the phone are recorded in WhatsApp Web storage during an active connection. If a user answers a video call or watches a video through the phone's application, information about the activity will be found on the computer. Because user actions in WhatsApp Messenger and the Web Application are stored in files that can be easily parsed and manipulated.

Although no conversations are stored directly in these files, someone's timeline of media files viewed and information about the time they spent with their computer can be easily discerned.

In searching for digital artifacts contained in WhatsApp Web, this research will use Sleuth Kit Autopsy tools, which can show copies of conversations and various media files such as audio, video, voice notes, images, and call history, as seen in the example figure 3 below:

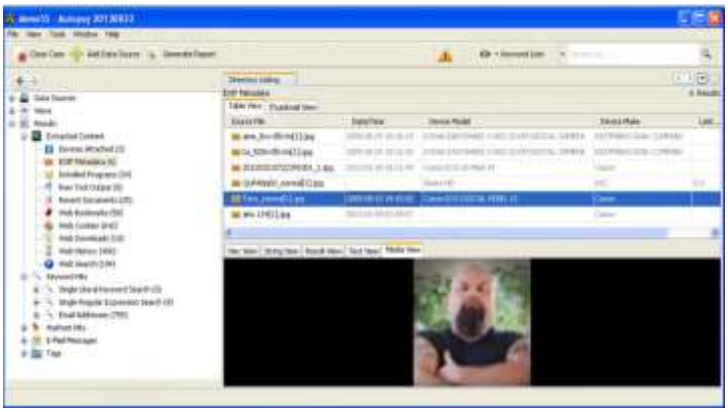

Fig. 3 Media File Extraction Using Autopsy

When analyzing media files, we need to check the integrity of the image by clicking the image integrity button and producing an md5 hash of the image. An important thing to note is that this hash should match the one we have

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 1, January 2023
https://doi.org/10.47709/cnahpc.v5i1.2286

Submitted : May 02, 2023
Accepted : May 22, 2023
Published : May 24, 2023

for the image at the beginning of the procedure. The image hash is important because it tells us whether the provided image has been tampered with or not.

Comparative data recovery analysis is a step-in data recovery that has been extracted using forensic tools such as TSK recover, Foremost, and Testdisk recovery. Data files such as JPG, PNG, and MP4 on flash drives, HDDs, SSDs, and other storage media that have been corrupted will be processed using data file recovery methods using several tools, which will find differences that affect data recovery on these tools so that they can be fully opened again.

Forensic Toolkit, or FTK, is a computer forensic software created by AccessData. It scans the hard drive and searches for various information. FTK also has the potential to find deleted emails and scan the disk for text strings to use as a password dictionary to crack encryption. To view avatars and other media files such as photos, videos, and more, you can use the FTK Imager application.

The analysis of media file extraction using Autopsy revealed significant insights into the artifacts created by the WhatsApp Web application. These artifacts serve the purpose of capturing comprehensive information about user actions, suggesting a deliberate design aimed at facilitating diverse methods of information gathering.

During an active connection, it appears that actions performed within the WhatsApp Messenger application on the user's phone are stored in WhatsApp Web storage. Consequently, activities such as answering video calls or watching videos through the phone's application leave traces of information on the connected computer. The storage files associated with both WhatsApp Messenger and the Web Application are structured in a way that allows for easy parsing and manipulation.

While the files themselves do not directly store conversations, they do provide valuable indications of a user's media file timeline and the duration of their interactions with the computer. By examining these files, it is possible to discern which media files were viewed and the corresponding timeframes.

To conduct the analysis of digital artifacts present in WhatsApp Web, the Sleuth Kit Autopsy tools were employed. These tools enable the retrieval of copies of conversations as well as various media files, including audio, video, voice notes, images, and call history. Figure 3 illustrates an example of media file extraction using Autopsy.

When analyzing media files, it is essential to verify the integrity of the images by using the image integrity button and generating an MD5 hash of the image. The image hash serves as a crucial reference point, allowing the determination of whether the provided image has been tampered with or remains unaltered.

Furthermore, a comparative data recovery analysis was performed on the extracted data using forensic tools such as TSK recover, Foremost, and Testdisk recovery. This analysis focused on processing data files, such as JPG, PNG, and MP4, found on various storage media like flash drives, HDDs, SSDs, and others. The aim was to employ data file recovery methods using multiple tools to identify discrepancies that impact data recovery, thereby enabling complete restoration of the affected files.

In addition to Autopsy, the Forensic Toolkit (FTK), developed by AccessData, was utilized as computer forensic software. FTK scans the hard drive and searches for a wide range of information. It possesses the capability to discover deleted emails and conduct disk scans for text strings, which can be used as a password dictionary for encryption cracking purposes. The FTK Imager application facilitates the viewing of avatars and other media files such as photos and videos. Figure 4 provides an overview of several artifacts that can be found using this tool.

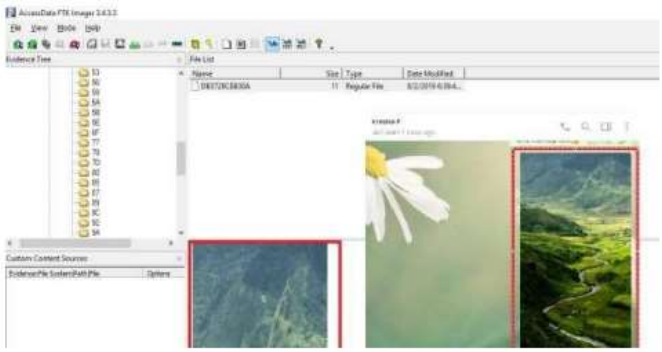

Fig. 4 Artifact Media File on FTK Imager

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 1, January 2023
https://doi.org/10.47709/cnahpc.v5i1.2286

Submitted : May 02, 2023
Accepted : May 22, 2023
Published : May 24, 2023

To search for other artifacts such as contact numbers stored in the WhatsApp database, we need a DB browser for SQLite to access the storage in the database. This is also to obtain all kinds of contact numbers, whether they are registered in WhatsApp or not.

We can also obtain information about user identities when accessing directories in XML format. The WhatsApp application automatically backs up all conversations to the SQLite database and stores them in the WhatsApp folder on the internal memory or SD card. The database file is then encrypted with crypt8 encryption. So when there are changes, WhatsApp will automatically back up all conversation history.

The analysis of the tools used revealed valuable findings in the search for artifacts within the WhatsApp database. To access the storage within the database and retrieve additional artifacts, a DB browser for SQLite was employed. This allowed for the extraction of contact numbers stored in the database, including those that are not registered in WhatsApp.

Furthermore, by accessing directories in XML format, it was possible to gather information about user identities. The WhatsApp application implements an automatic backup mechanism that stores all conversations in the SQLite database, which is then saved in the WhatsApp folder on the internal memory or SD card. Notably, the database file is encrypted using crypt8 encryption. Consequently, whenever changes occur, WhatsApp automatically creates a backup of the entire conversation history.

These findings highlight the significance of the WhatsApp database as a valuable source of information. By leveraging the DB browser for SQLite and examining the directories in XML format, investigators can extract contact numbers and gain insights into user identities. Additionally, the automatic backup mechanism ensures that a comprehensive record of conversation history is available, offering potential avenues for further analysis and investigation.

3.4 Reporting

The reporting phase in web forensics analysis of WhatsApp application on the latest browser version using the NIST framework involves preparing an accurate and legally acceptable digital forensic analysis report. This phase involves processing the results of the previous forensic analysis phase and creating a report that explains the results of the digital forensic analysis that has been carried out.

The results of the testing using the NIST framework were successful in analyzing digital artifacts on the WhatsApp browser, such as conversations, connected and disconnected contact numbers on the WhatsApp application, media files, several conversations in WhatsApp storage, and most importantly, an encrypted database file. The applied database extraction process also successfully extracted some conversations stored in internal or external memory using WhatsApp extractor and decryptor to convert the backup database into a text database that can be viewed in the SQLite database browser. This phase can open deleted conversations based on the data that has been automatically backed up by the WhatsApp application or manual backup.

The analysis report of the web forensics investigation on the latest version of the WhatsApp application, conducted using the NIST framework, focuses on preparing a comprehensive and legally acceptable digital forensic analysis report. This report encompasses the processing of the findings from the previous forensic analysis phase and aims to provide a clear explanation of the results obtained through the digital forensic analysis.

The testing carried out using the NIST framework yielded successful results in analyzing various digital artifacts within the WhatsApp browser. These artifacts included conversations, both active and inactive contact numbers associated with the WhatsApp application, media files, multiple conversations stored in the WhatsApp storage, and notably, an encrypted database file.

The extraction process applied to the database proved to be effective, enabling the retrieval of some conversations stored in the internal or external memory. This was achieved using a WhatsApp extractor and decryptor, which successfully converted the backup database into a text database that could be viewed using a SQLite database browser. Consequently, this phase allowed for the recovery and examination of deleted conversations based on the data automatically backed up by the WhatsApp application or through manual backups.

The findings of this analysis report provide substantial evidence of the forensic examination conducted on the WhatsApp application. It demonstrates the successful extraction and analysis of digital artifacts, such as conversations and media files, as well as the ability to access and interpret data stored in the encrypted database. The information

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 1, January 2023
https://doi.org/10.47709/cnahpc.v5i1.2286

Submitted : May 02, 2023
Accepted : May 22, 2023
Published : May 24, 2023

obtained through this analysis contributes significantly to the investigation and facilitates a comprehensive understanding of the user's interactions and activities within the WhatsApp application.

4. CONCLUSION

With several stages of the NIST framework used in this study, it was successful in analyzing digital artifacts on the WhatsApp browser. Based on the research results using open-source-based tools, one of the data recovery stages is the result of the acquisition of several recovery tools that have been tested in this study. Data files such as JPG, PNG, and MP4 that are damaged or corrupted have been recovered with existing forensic tools. It can be concluded that among these tools, some can recover damaged data files and can be opened completely, while others cannot. This study also examined artifacts stored for WhatsApp Web. Two hypotheses were made for the examination: Storage can be forensically examined, and significant artifacts for WhatsApp Web application, and WhatsApp Web application artifacts can be used to create a timeline analysis in forensic investigations. A quasi-experimental pretest-posttest single-case design was conducted to evaluate the remaining artifacts in Storage I by the application. The results show that Storage I is a valuable source of information for forensic investigations when analyzed specifically for WhatsApp Web application. Information based on the suspect's actions was detected to be suitable for utilization in forensic presentation of indexed timeline evidence. Therefore, both hypotheses made for this study proved to be correct.

5. SUGGESTIONS

WhatsApp always updates its encryption standards to continuously protect against illegal access. This presents a challenge for forensic investigators to keep up with these developments, especially those related to WhatsApp databases, to ensure that they can still encrypt the databases on WhatsApp Web. This research still uses Crypt8, and every update, WhatsApp may use Crypt9 or even Crypt10. Therefore, forensic investigators should further study the features of WhatsApp in the future. The NIST framework used in this research has successfully analyzed digital artifacts on WhatsApp currently, but in the future, there may be other frameworks that can accommodate the needs of analyzing digital artifacts on the WhatsApp browser. From this research, we can also see that the comparison analysis of the tools used for data recovery is important for forensic experts. If they encounter a case of lost or damaged files, they should not rely on just one tool, but try all available forensic tools. This research showed that some tools were able to recover files perfectly while others were not.

6. REFERENCES

Iqbal, M., & Riadi, I. (2019). Forensic WhatsApp based Android using National Institute of Standard Technology (NIST) Method. *International Journal of Computer Applications*, *177*(8). https://doi.org/10.5120/ijca2019919443

Jafri, M. S., Raharjo, S., & Arief, M. R. (2022). Implementation of ACPO Framework for Digital Evidence Acquisition in Smartphones. *CCIT Journal*, *15*(1). https://doi.org/10.33050/ccit.v15i1.1586

Khweiled, R., & Jazzar, M. (2021). An Improved Framework For cyberbullying Investigation Process on WhatsApp application. *Journal of Xi'an University of Architecture & Technology*, *XIII*(9).

Lakshmi, M. S. P., & Rajeshrajesh, P. (2019). A forensic approach to perform android device analysis. *International Journal of Recent Technology and Engineering*, *7*(6).

Martínez-Comeche, J. A., & Ruthven, I. (2023). Informational features of WhatsApp in everyday life in Madrid: An exploratory study. *Journal of Information Science*, *49*(1). https://doi.org/10.1177/0165551521990612

Montasari, R., Hill, R., Carpenter, V., & Montaseri, F. (2018). Digital Forensic Investigation of Social Media, Acquisition and Analysis of Digital Evidence. *International Journal of Strategic Engineering*, *2*(1). https://doi.org/10.4018/ijose.2019010105

Paligu, F., Kumar, A., Cho, H., & Varol, C. (2019). BrowStExPlus: A Tool to Aggregate IndexedDB Artifacts for Forensic Analysis. *Journal of Forensic Sciences*, *64*(5). https://doi.org/10.1111/1556-4029.14043

Qureshi, M. A., & El-Alfy, E. S. M. (2019). Bibliography of digital image anti-forensics and anti-anti-forensics techniques. In *IET Image Processing* (Vol. 13, Issue 11). https://doi.org/10.1049/iet-ipr.2018.6587

Riadi, I., & Firdonsyah, A. (2018). Forensic analysis of android-based instant messaging application. *Proceeding of 2018 12th International Conference on Telecommunication Systems, Services, and Applications, TSSA 2018*.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 1, January 2023
https://doi.org/10.47709/cnahpc.v5i1.2286

Submitted : May 02, 2023
Accepted : May 22, 2023
Published : May 24, 2023

https://doi.org/10.1109/TSSA.2018.8708798

Rosselina, L., Suryanto, Y., Hermawan, T., & Alief, F. (2020). Framework design for the retrieval of instant messaging in social media as electronic evidence. *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, *2020-October*. https://doi.org/10.23919/EECSI50503.2020.9251888

Shah, Z., Kyaw, A., Truong, H. P., Ullah, I., & Levula, A. (2022). Forensic Investigation of Remnant Data on USB Storage Devices Sold in New Zealand. *Applied Sciences (Switzerland)*, *12*(12). https://doi.org/10.3390/app12125928

Simanjuntak, M. S., & Panjaitan, J. (2021). Analisa Recovery Data Menggunakan Software. *Jurnal Teknik Informatika Komputer Universal*, *1*(1).

Vukadinovic, N. V. (2019). WhatsApp Forensics: Locating Artifacts in Web and Desktop Clients. *Master's Thesis, Purdue University Graduate School*, *May*.

Wijnberg, D., & Le-Khac, N. A. (2021). Identifying interception possibilities for WhatsApp communication. *Forensic Science International: Digital Investigation*, *38*. https://doi.org/10.1016/j.fsidi.2021.301132

Zuhriyanto, I., Anton Yudhana, & Imam Riadi. (2020). Comparative analysis of Forensic Tools on Twitter applications using the DFRWS method. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(5). https://doi.org/10.29207/resti.v4i5.2152

* Corresponding author